

PTH:MWG  
F.#2019R1370

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
AN APPLE IPHONE X, SERIAL NO.  
357280096349524, CURRENTLY  
LOCATED IN THE EASTERN DISTRICT  
OF NEW YORK

APPLICATION FOR A SEARCH  
WARRANT FOR AN ELECTRONIC  
DEVICE

Case No. 20-MJ-557

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Steven Mullen, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”), and am assigned to the Child Exploitation Investigations Unit. I have been a Special Agent for twelve years. My responsibilities include investigations of cases involving the promotion of a sexual performance by a child through the use of electronic devices and the internet, possession and distribution of child pornography through the use of electronic devices and the internet,

human trafficking and other incidents of the exploitation of children on the internet. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my training and experience, I also have gained expertise in the identification of minor victims. As part of my responsibilities, I have been involved in the investigation of numerous child pornography and child exploitation cases.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is a gold Apple iPhone X, serial number 357280096349524, hereinafter the “Device.” The Device is currently in a locked case in the possession of my colleague within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

### **DEFINITIONS**

6. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

- a. The terms “minor,” “sexually explicit conduct” and “visual depiction,” are defined as set forth in Title 18, United States Code, Section 2256; and
- b. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . .”<sup>1</sup>

### **PROBABLE CAUSE**

7. In June 2019, HSI began investigating VICTOR HUGO GALARZA for sex tourism in violation of 18 U.S.C. § 2423. During the course of the investigation, HSI developed probable cause to believe that GALARZA has produced, possessed and distributed child pornography, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A.

---

<sup>1</sup> See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

8. During the course of that investigation, several devices belonging to GALARZA, including multiple phones and a computer, were seized and searched pursuant to the border search doctrine and search warrants.

9. During searches of a seized phone (hereinafter “GALARZA’s Phone-1”), law enforcement recovered four video files depicting another adult individual (hereinafter “Co-Conspirator-1”), engaging in sexual activity with a minor individual (hereinafter “Victim-1”), who was sixteen years old at the time. GALARZA’s voice can be heard on the video files directing Co-Conspirator-1 and Victim-1 to engage in specific sexual acts.

10. On or about June 7, 2019, GALARZA exchanged messages via WhatsApp with another individual (hereinafter “Co-Conspirator-2”), concerning a time to meet Victim-1. Specifically, on or about June 7, 2019, at approximately 9:09 a.m., GALARZA wrote to Co-Conspirator-2: “[Victim-1] is set 1 pm[.] Miro Girls set 7 pm[.]” Later that day, at approximately 11:13 a.m., GALARZA wrote to Co-Conspirator-2: “See you at 1pm[.] [Victim-1] is set.”

11. At approximately 12:35 p.m., GALARZA sent Victim-1 a text message with a certain address in Medellin, Colombia (the “Medellin Location”).

12. Metadata for the four above-described video files shows that the video files were created on June 7, 2019, between approximately 3:07 p.m. and approximately 3:20 p.m. at the Medellin Location.

13. Law enforcement agents, including myself, interviewed Victim-1 on or about September 26, 2019. Victim-1 stated that she was sixteen years old at that time.<sup>2</sup> Victim-1 positively identified a photograph of GALARZA as “Victor.” Victim-1 explained, in sum and substance and in part, that “Victor” paid her approximately one million Colombian pesos in cash to have sex with Co-Conspirator-1 while “Victor” remained in the room. After being shown photographs of the Medellin Location, Victim-1 positively identified the Medellin Location as the place where she was paid by “Victor” to have sex with Co-Conspirator-1. Victim-1 also identified herself in a still photograph from one of the video files created on June 7, 2019, that was recovered from GALARZA’s Phone-1.

14. Victim-1 also reported to law enforcement agents, including myself, that she met Co-Conspirator-2 through GALARZA and that she had sex with Co-Conspirator-2 on multiple occasions in exchange for money.

15. On October 8, 2019, the Honorable Peggy Kuo, United States Magistrate Judge for the Eastern District of New York, signed an arrest warrant for GALARZA based upon a complaint charging GALARZA with having violated 18 U.S.C. § 2251 (production of child pornography). See 19-MJ-908.

16. HSI agents, including myself, arrested GALARZA the next day at his home in Queens, New York. Thereafter, GALARZA was detained and advised of his Miranda rights.

---

<sup>2</sup> HSI agents have obtained a copy of Victim-1’s birth certificate, which confirms that Victim-1 was sixteen years old at the time of the interview.

GALARZA waived his Miranda rights and agreed to speak with law enforcement. After waiving his Miranda rights, GALARZA made the following statements, in sum and substance and in part, which were audio recorded by HSI. GALARZA admitted that he had produced approximately thirty to forty pornographic videos of Co-Conspirator-1 engaging in sexual activity with young females in Colombia, that he did so over a period of approximately eight years and that he sold electronic copies of such videos to friends in exchange for payments via PayPal. GALARZA further stated in his post-arrest interview that he arranged for Co-Conspirator-2, a United States citizen, to have sex with a fifteen-year-old girl in Colombia.

17. GALARZA informed me that he had known Co-Conspirator-2 for approximately twelve years.

18. HSI found evidence of additional minor victims on GALARZA's devices. - Searches of GALARZA's Phone-1 revealed conversations between GALARZA and Co-Conspirator-2 appearing to discuss sex with underage girls. On June 7, 2019, GALARZA sent a photo of a young female to Co-Conspirator-2 and wrote the following messages:

15 yrs old  
Raw dog  
Out of farm system  
For tonight ?

Co-Conspirator-2 responded: "Hell fucking yes" and "You know I want that." GALARZA responded in a voice message, in sum and substance and in part, that this girl had a twin sister, reiterating that the sisters were fifteen years old. In another voice message sent shortly

thereafter, GALARZA stated in part, “the two twins, the fifteen years olds, they know they are coming to get fucked.” In addition, GALARZA’s phone contains a recording of an individual other than GALARZA having sex with two girls who appear to be twins and, based on my training and experience, appear to be minors.

19. On August 20, 2019 GALARZA sent Co-Conspirator-2 an audio message on another device (hereinafter “GALARZA Phone-3”) stating that they could not “do tenders” for a few days because Co-Conspirator-2’s brother was visiting and the brother is “very strict about over 18.” GALARZA went on to say that they would have to “sacrifice” themselves for those three or four days. Co-Conspirator-2 responded, “Shitttttt you sacrifice imma just lie And be like she 18[.] Fuck that 3 days no tenders.” Based on my training and experience and the context of these conversations, I understand GALARZA and Co-Conspirator-2 to be discussing sex with individuals under the age of eighteen.

20. In another conversation, Co-Conspirator-2 said he had oral sex with a girl who said she was sixteen years old, and GALARZA responded that the girl was actually fifteen.

21. One individual (hereinafter “Individual-4”) reported to me and other law enforcement agents, in sum and substance and in part, that, in May and August of 2014, when she was sixteen years old, she was paid to engage in sex with GALARZA while in Colombia. Individual-4 reported that GALARZA set her up to have sex with Co-Conspirator-2 as well, and offered her money to engage in sex with a third individual. She stated that she had sex with the third individual and believes GALARZA recorded those sexual encounters. All of these sexual encounters occurred in Colombia.

22. Often, in conversations with Co-Conspirator-2, GALARZA and Co-Conspirator-2 discuss the price of girls in Colombian pesos.

23. On or about September 26, 2019, I called the number in GALARZA's devices associated with Co-Conspirator-2. I greeted the man who answered the phone by Co-Conspirator-2's first name. He did not deny that was his name and I recognize the voice as that of Co-Conspirator-2 from later conversations with Co-Conspirator-2.

24. On or about October 9, 2019, Co-Conspirator-1, who is a resident of Colombia, and Co-Conspirator-2, who is a United States citizen residing in Colombia, were arrested by Colombian authorities and charged with offenses related to the sexual exploitation of children. Co-Conspirator-2 is also charged with possession of an illegal firearm. GALARZA has been indicted in the Eastern District of New York and charged with, among other crimes, conspiracy to sexually exploit a minor. See United States v. Victor Hugo Galarza, Criminal Docket No. 19-508 (BMC), ECF Docket No. 12.

25. The Device was seized from Co-Conspirator-2 upon his arrest in Colombia. Colombian authorities have informed me that they searched Co-Conspirator-2's home after his arrest and did not find any additional phones.

26. After his arrest, I interviewed Co-Conspirator-2 while he was in jail in Colombia. I asked him for the password to his phone, which he refused to provide, stating in sum and substance that we would not be able to get into his phone. During that conversation, Co-Conspirator-2 acknowledged that he has spoken to me during the September 26, 2019, telephone call referenced above.



27. Based on the foregoing, there is probable cause to believe that the Device is Co-Conspirator-2's primary phone and the phone used to communicate with GALARZA, as discussed above.

28. Based on my training and experience, I also know that criminals frequently use cellphones such as the Device to communicate about criminal conduct and to store photographs, videos and other records that would be evidence of criminal conduct. In particular, just as non-criminals frequently use cellphones to communicate and coordinate plans with others, participants in conspiracies to sexually exploit children often use cellphones to communicate with co-conspirators and to store the names and contact information of co-conspirators and victims. In addition, individuals who possess or create child pornography often store that child pornography on their cellphones.

29. Similarly, just as non-criminals use cellphones to search the internet for matters of interest to them, possessors, distributors and creators of child pornography commonly use cellphones such as the Device to search or browse the internet for information relating to child pornography and their criminal conduct.

30. Based on the foregoing facts and my training and experience, there is probable cause to believe that the Device contains evidence of the crimes discussed herein.

31. The Device is currently in the lawful possession of HSI. It came into HSI's possession in the following way: incident to Co-Conspirator-2's arrest in Colombia, the Colombian authorities seized the Device from Co-Conspirator-2. The Colombian authorities later provided the Device to HSI. Therefore, while HSI might already have all necessary

authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

32. The Device is currently in a locked case in the possession of my colleague within the Eastern District of New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the HSI.

### **TECHNICAL TERMS**

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail;

taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any

digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and

receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

34. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and/or PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file).

- i. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- k. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- l. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

38. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

39. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.


### **REQUEST FOR SEALING**

1. It is respectfully requested that this Court issue a limited order, sealing until further order of the Court, all papers submitted in support of this application and search warrant, but allowing the government to disclose the application and warrant to the defendant charged in United States v. Victor Hugo Galarza, Criminal Docket No. 19-508 (BMC). I believe that the limited sealing of these documents is necessary because the warrant is

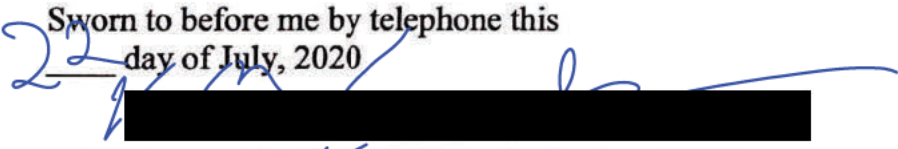


relevant to an ongoing investigation that is not known to all of the targets of the investigation at this time, including those individuals with whom GALARZA may have shared child pornography. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

  
\_\_\_\_\_  
Steven Mullen  
Special Agent  
United States Department of Homeland Security  
Homeland Security Investigations  
Child Exploitation Investigations Unit

Sworn to before me by telephone this  
22 day of July, 2020

  
\_\_\_\_\_  
Honorable Vera M. Scanlon  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

The property to be searched is a gold Apple iPhone X, serial number 357280096349524, hereinafter the “Device.” The Device is currently in a locked case in the possession of my colleague within the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 2251, 2252, 2252A and 2243 and involve VICTOR HUGO GALARZA and/or his co-conspirators, including Co-Conspirators-1 and -2, since January 1, 2012, including:

- a. Records and information pertaining to the receipt, distribution, purchase, production, possession or solicitation of child pornography, including communications with minors or purported minors evidencing an effort to persuade, entice, induce or coerce them into producing or creating child pornography, as well as images of child pornography and motion pictures, films, videos and other recordings of visual depictions of minors engaged in sexually explicit conduct;
- b. Records and information pertaining to sex tourism, including communications with minors or purported minors evidencing an effort to persuade, entice, induce or coerce them into engaging in sexually explicit conduct;
- c. Evidence of the identities and whereabouts of any minors or purported minors referenced in (a) and (b);
- d. Records and information pertaining to the transportation of any visual depiction of a minor engaged in sexually explicit conduct to the United States;

- e. Communications with individuals who have reported that when they were minors they engaged in sexually explicit conduct with GALARZA or his co-conspirators, or individuals who law enforcement officials have identified as potential victims;
- f. Communications by, among and between co-conspirators, including the co-conspirators identified herein, as well as any potential purchasers of child pornography;
- g. Records and information pertaining to the identity of any persons who communicated with the Device about matters relating to the solicitation, production, distribution or purchase of child pornography or the sexual exploitation of minors, including records that help reveal their identities and whereabouts;
- h. Records and information regarding GALARZA and/or his co-conspirators' travel, location or schedule, including records evidencing the use of any relevant Internet Protocol addresses;
- i. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- j. Records and information concerning any Internet accounts used to possess, receive or distribute child pornography; and
  - k. Records and information pertaining to financial transactions relating to the production, sale or possession of child pornography or the sexual exploitation of a child, including bank records, checks, credit card bills, account information and other financial records.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.